King Fahd University of Petroleum & Minerals
Information and Computer Science Department

ICS254 (Discrete Structures II))

Term: 172

Implementation of the Diffie-Hellman Protocol Programming Assignment Report

Group #6

Doctor in Charge:
Dr. Wasfi AlKhteeb

Group Members:

Name	ID
Yousef Majeed	201568070
Thamer Mashni	201417240

Saturday, April 28, 2018

"Group #07" ® - *"Success is a journey not a destination!"*

Table of Contents

Implementation of the Diffie-Hellman Protocol

1. The objective(s) of the protocol

To make two parties able to exchange a secret key over an insecure communications channel without having shared any information in the past.

2. How and under which restrictions/environment does it work?

- A sender and a receiver need to share a common key
- First the sender and the receiver agree to use a prime p and a primitive root a of p.
- Then the sender chooses a secret integer k1 and sends $a^{k1}\,\boldsymbol{mod}\,p$ to the receiver .
- The receiver chooses a secret integer k_2 and sends $a^{k2}\,\boldsymbol{mod}\,p$ to the sender
- The sender computes $(a^{k2})^{k1}\,\boldsymbol{mod}\,p$
- The receiver computes $(a^{k1})^{k2}\,\boldsymbol{mod}\,p$
- At the end of this protocol, sender and receiver have computed their shared key, namely $(a^{k2})^{k1}\,\boldsymbol{mod}\,p = (a^{k1})^{k2}\,\boldsymbol{mod}\,p$.

3. Public Information and Private Information

3.1 Information can be made Public:

a) p
b) a
c) $a^{k1}\,\boldsymbol{mod}\,p$ = A
d) $a^{k2}\,\boldsymbol{mod}\,p$ = B

3.2 Information can be made Private:

a) k_1
b) k_2
c) and the common key $(a^{k2})^{k1}\,\boldsymbol{mod}\,p = (a^{k1})^{k2}\,\boldsymbol{mod}\,p$

4. References

- Kenneth, H. *Discrete Mathematical and its Applications, Seventh Edition*, course Textbook.

5. How to compile and run the code

We have implemented the application with simple user interface to facilitate working and testing the application as shown in part 7. First you choose the desired operation (using the protocol or cracking protocol), then enter the required input for the operation then click on compute button (or crack) to show the result.

6. Specific details of the algorithms that have been implemented

Regarding to the BONUS part, we have implemented the discrete logarithm algorithm to break the security of the Diffie-Hellman protocol, so the algorithm says:

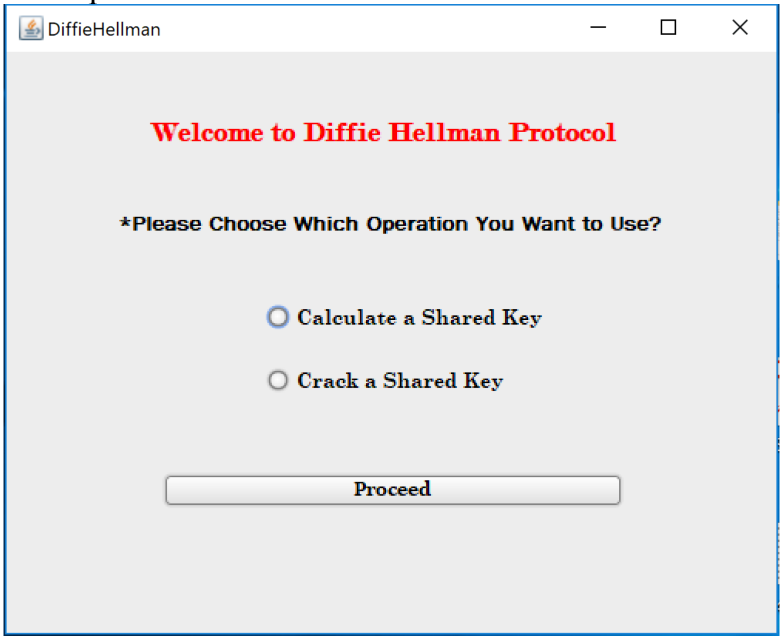
Suppose that p is a prime, r is a primitive root modulo p, and a is an integer between 1 and $p - 1$ inclusive. If $r^e \boldsymbol{mod}\, p = a$ and $0 \leq e \leq p - 1$, we say that e is the *discrete logarithm* of a modulo p to the base r and we write $\log_r a = e$ (where the prime p is understood).

So, it is clear that is can be worked with our case where the public information will be placed in the equation to find the private keys then after that, calculate the shared secret key will be done.
'p' is the same name of our prime
'r' is the primitive root = 'a' in our implementation
'a' is the public key = 'A' and 'B' in our implementation
'e' is the private key = 'k1' and 'k2' in our implementation
so, the equations will be:
$a^{k1} \boldsymbol{mod}\, p = A$
$a^{k2} \boldsymbol{mod}\, p = B$

7. Sample runs of the program

Application interface:

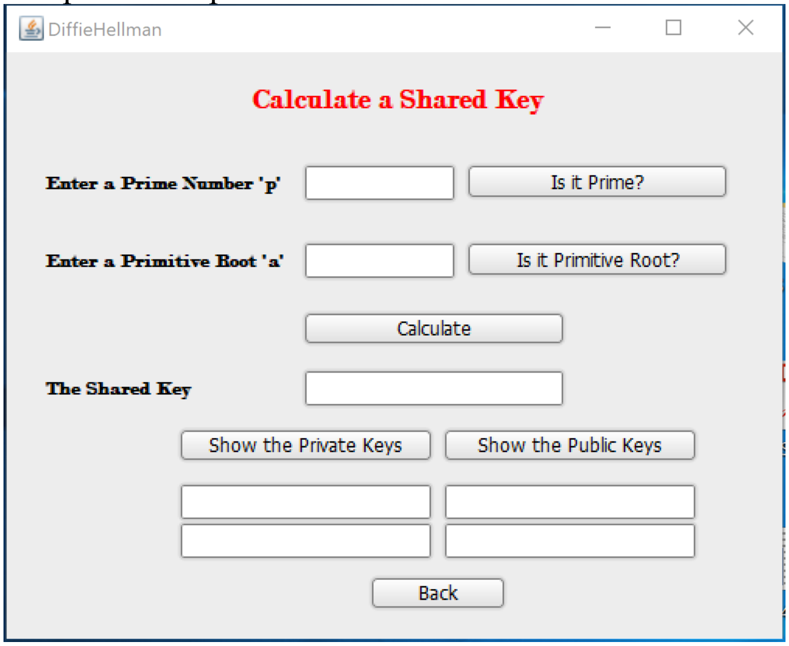
home panel:



Welcome to Diffie Hellman Protocol

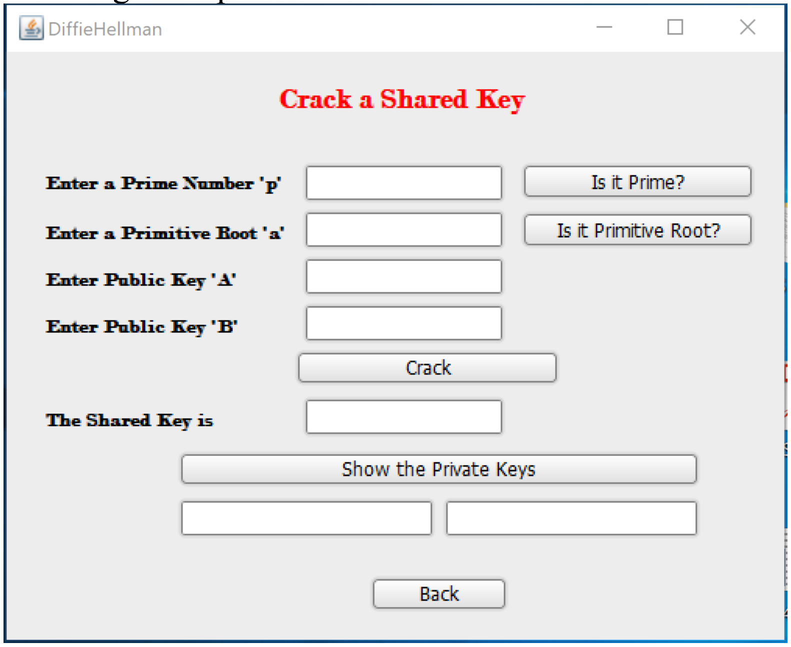
*Please Choose Which Operation You Want to Use?

compute DHP panel:



Calculate a Shared Key

Cracking DHP panel:



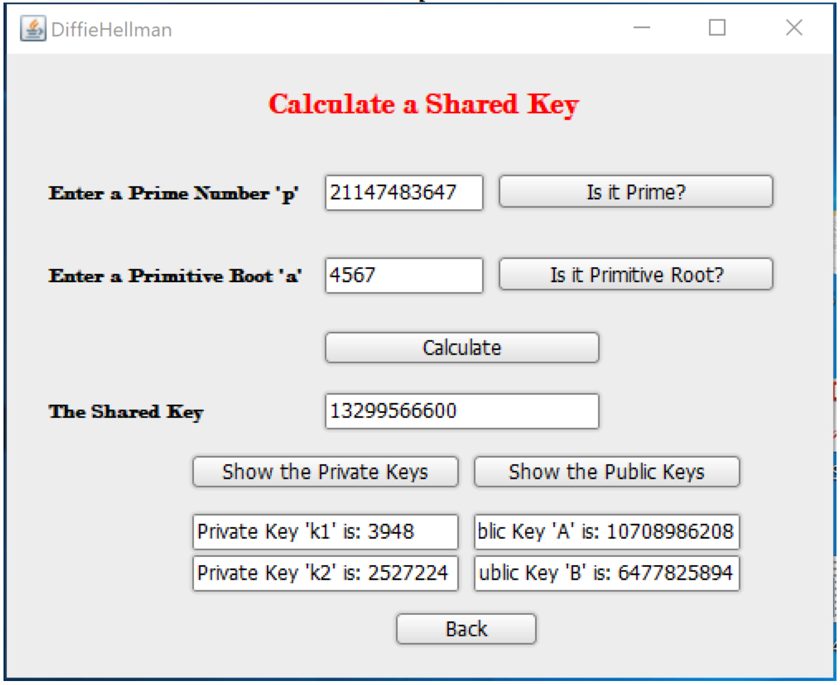
Valid Runs:

a- For compute DHP

1. since MAX_VALUE= 2147483647

   p = prime number larger than Integer.MAX_VALUE = 21147483647

   a = PRIMITIVE ROOT of p = 4567



Enter a Prime Number 'p' 21147483647

Enter a Primitive Root 'a' 4567

The Shared Key 13299566600

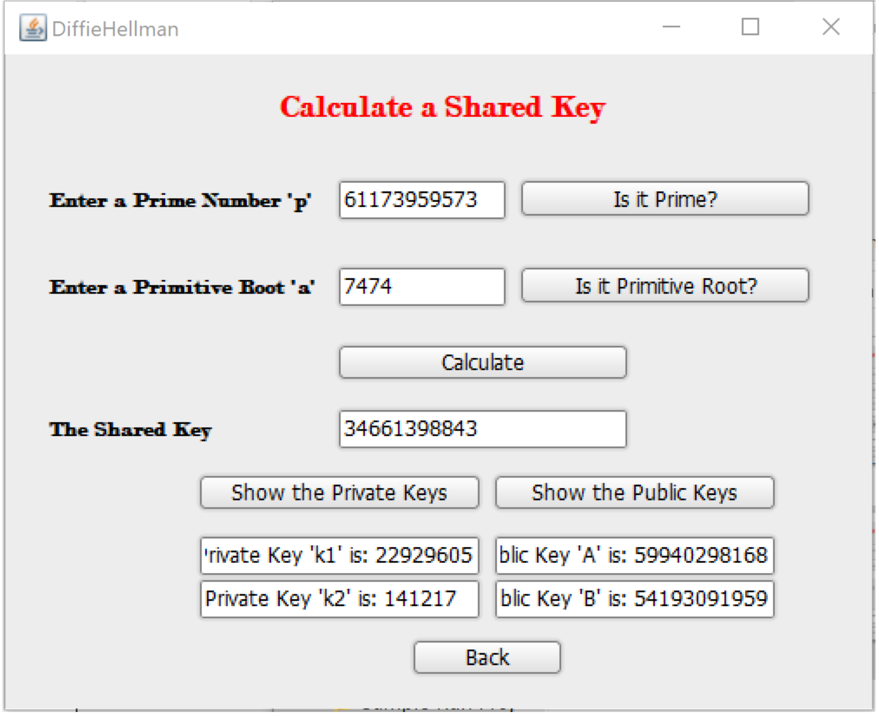
Private Key 'k1' is: 3948

Private Key 'k2' is: 2527224

blic Key 'A' is: 10708986208

ublic Key 'B' is: 6477825894

2. Another valid run with $p = 61173959573$, $a = 7474$



Calculate a Shared Key

Enter a Prime Number 'p' 61173959573

Enter a Primitive Root 'a' 7474

The Shared Key 34661398843

'rivate Key 'k1' is: 22929605

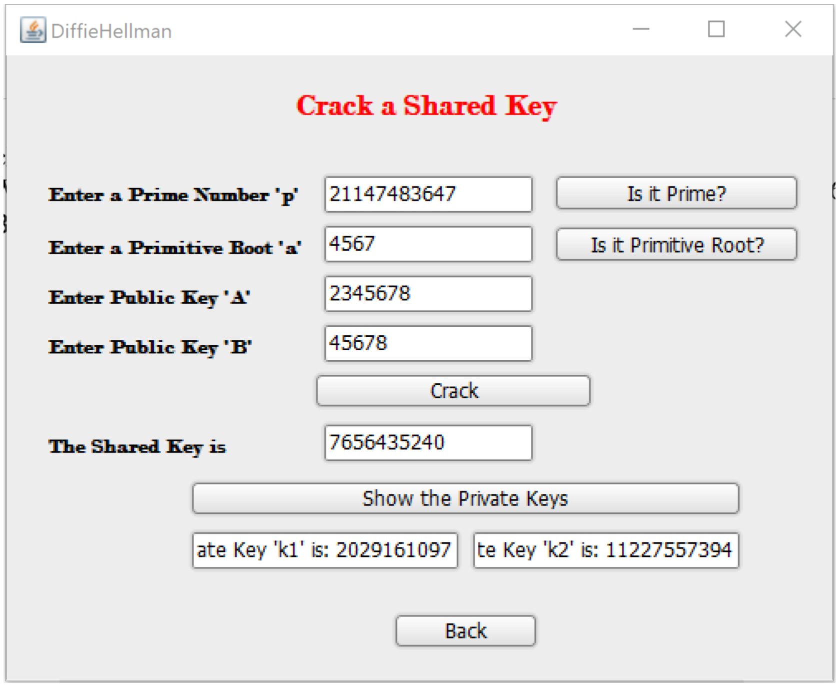
Private Key 'k2' is: 141217

blic Key 'A' is: 59940298168

blic Key 'B' is: 54193091959

2) For Cracking DHP

1. With $p = 21147483647$ and $a = 4567$ and randomly entered A = 2345678 & B=45678



Crack a Shared Key

Enter a Prime Number 'p' 21147483647

Enter a Primitive Root 'a' 4567

Enter Public Key 'A' 2345678

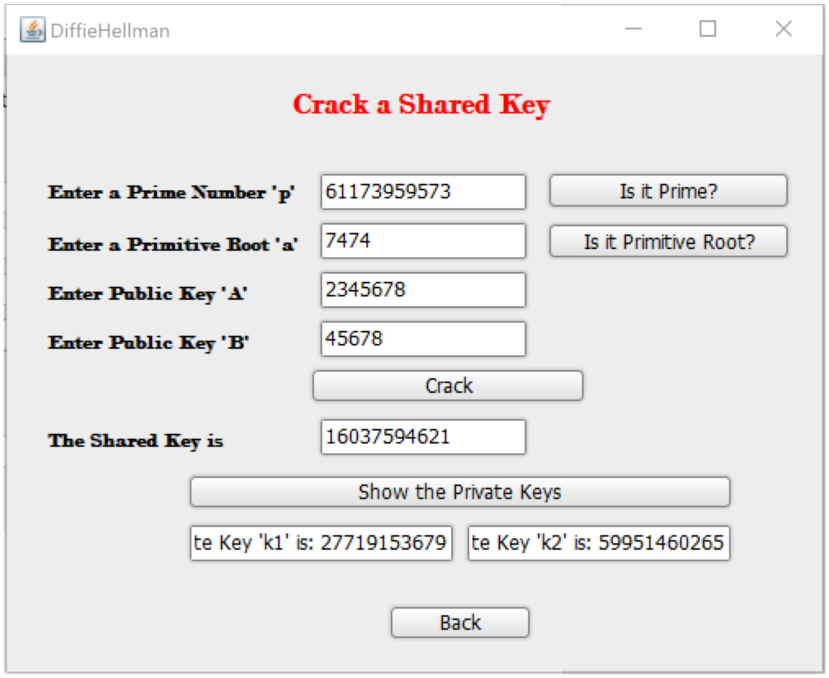
Enter Public Key 'B' 45678

The Shared Key is 7656435240

ate Key 'k1' is: 2029161097

te Key 'k2' is: 11227557394

2. Another run with $p = 61173959573$ and $a = 7474$ and randomly entered A = 2345678 & B = 45678


DiffieHellman

Crack a Shared Key

Enter a Prime Number 'p' 61173959573

Enter a Primitive Root 'a' 7474

Enter Public Key 'A' 2345678

Enter Public Key 'B' 45678

The Shared Key is 16037594621

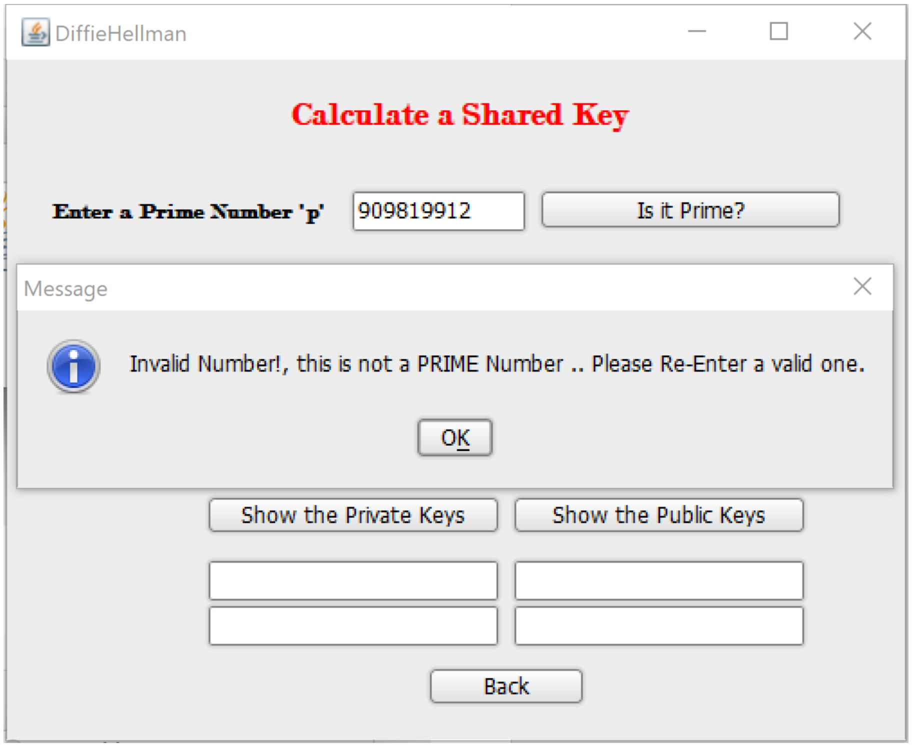
te Key 'k1' is: 27719153679

te Key 'k2' is: 59951460265

Invalid Runs:

a- For compute DHP

1.


DiffieHellman

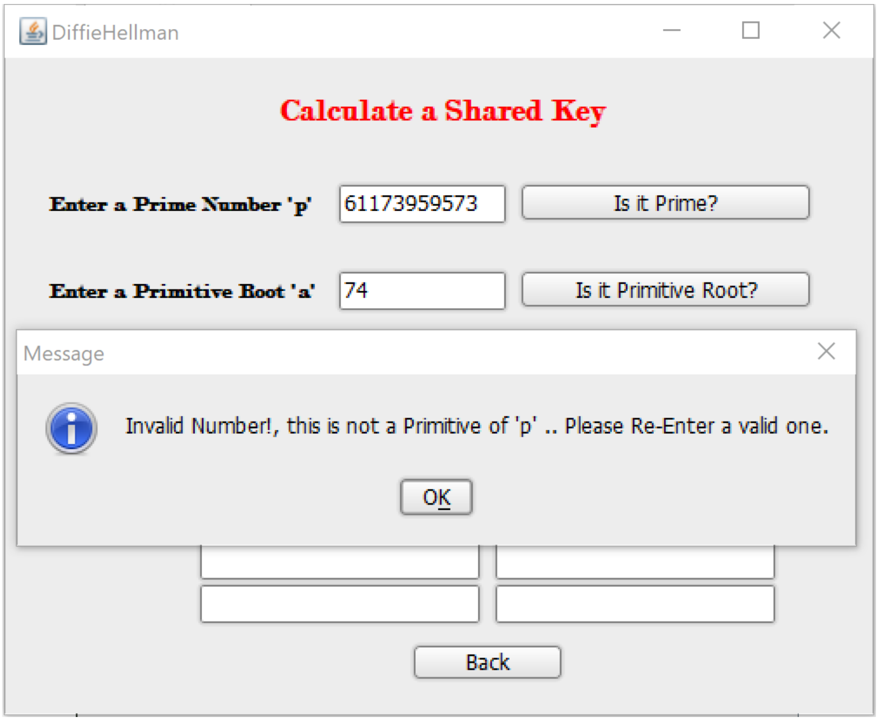
Calculate a Shared Key

Enter a Prime Number 'p' 909819912

Message

Invalid Number!, this is not a PRIME Number .. Please Re-Enter a valid one.

2.



Calculate a Shared Key

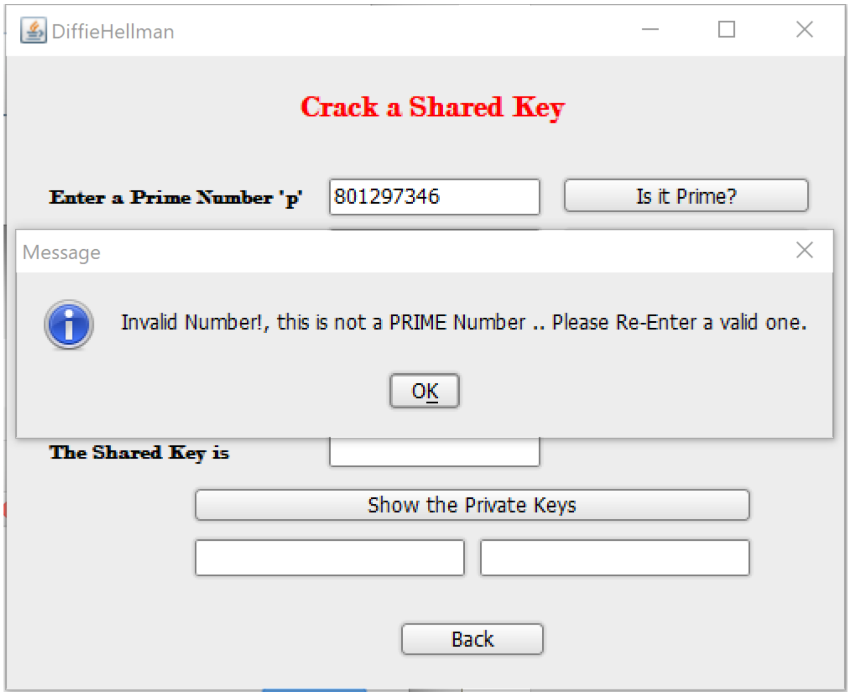
Enter a Prime Number 'p' 61173959573

Enter a Primitive Root 'a' 74

Invalid Number!, this is not a Primitive of 'p' .. Please Re-Enter a valid one.

b- For Cracking DHP

1.



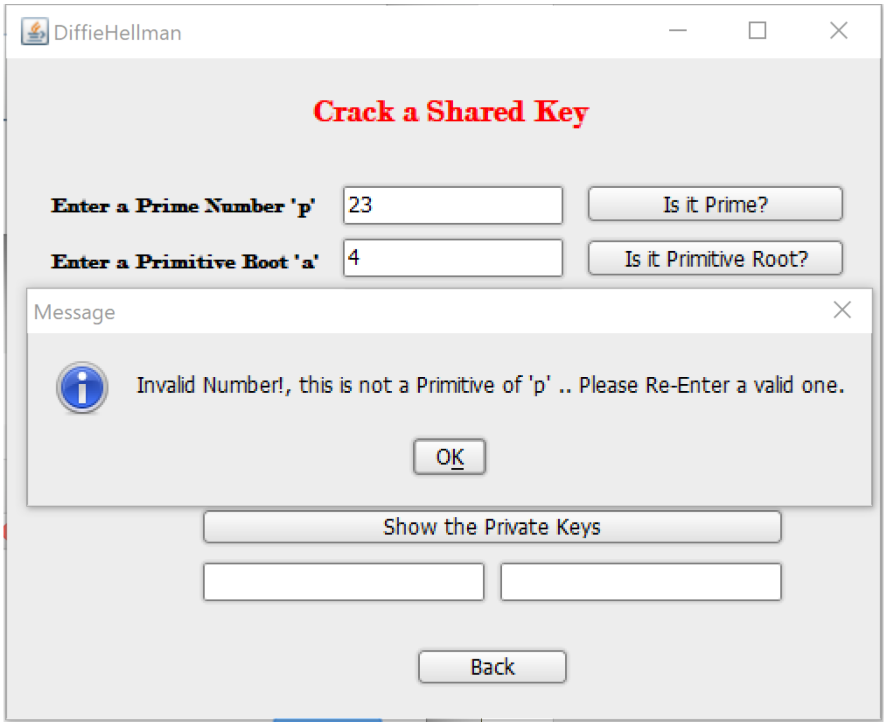
Crack a Shared Key

Enter a Prime Number 'p' 801297346

Invalid Number!, this is not a PRIME Number .. Please Re-Enter a valid one.

The Shared Key is

2.

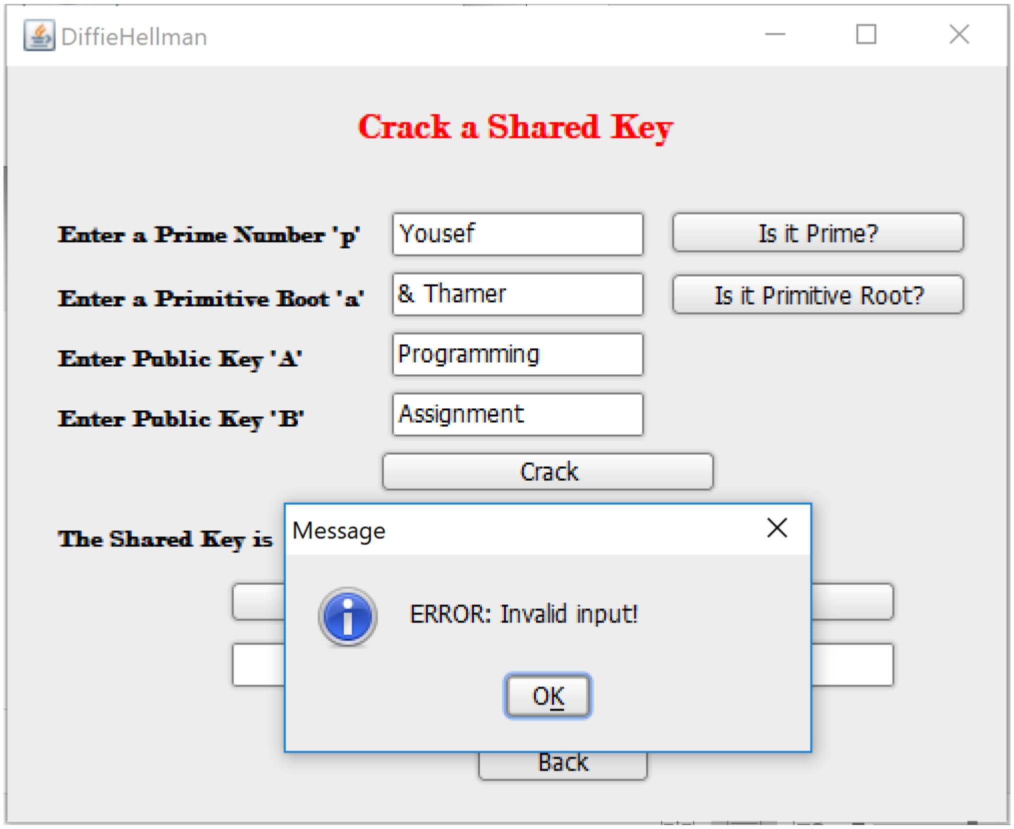


Enter a Prime Number 'p' 23

Enter a Primitive Root 'a' 4

Invalid Number!, this is not a Primitive of 'p' .. Please Re-Enter a valid one.

c- Invalid input Format



Enter a Prime Number 'p' Yousef

Enter a Primitive Root 'a' & Thamer

Enter Public Key 'A' Programming

Enter Public Key 'B' Assignment

The Shared Key is

ERROR: Invalid input!

8. Work Distribution

TASK RECORD

Date	Member	Task Details
18 April 2018	Thamer Mashni	Starting the project, do some most initial functions
22 April 2018	Yousef Majeed	Working on the main functionality of the program
24 April 2018	Yousef Majeed	Start working on the Bonus part and close to finish it
25 April 2018	Thamer Mashni	Make the program as a GUI Program
27 April 2018	Yousef Majeed	Enhance the GUI Program a little
28 April 2018	Both Members	Finalize Work and Finalize the Report